UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/975,815	10/11/2001	Neal A. Krawetz	10019968-1	9182

7590 11/16/2007

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
COLIN, CARL G	
ART UNIT	**PAPER NUMBER**
2136	
MAIL DATE	**DELIVERY MODE**
11/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/975,815	KRAWETZ, NEAL A.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 August 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 8/21/2007, applicant amends claim 33, the following claims 1-34 are presented for examination.

1.1 Applicant's remarks, pages 8-12, filed on 8/21/2007, with respect to the rejection of claims 1-34 have been fully considered but they are moot in view of a new ground of rejection.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-2, 4-8, 11-17, 19, 21-34 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 6,751,736 to **Bowman et al**.

As per claim 1, Bowman et al discloses a method for secure data transmission, comprising: generating a character string (random string) at a sender (see column 7, lines 25-29); generating a hash key (key (SHAD)) using the character string (random string) and a private key (secret string) (see column 7, lines 29-43); encrypting the data (VBC message string) using the hash key (see co7, lines 41-45); and transmitting an identification key (secret ID) associated with the sender, the character string (random string), and the encrypted data (encrypted VBC) from the sender to a recipient (see column 8, lines 18-22 and column 7, lines 57-62).

As per claim 2, Bowman et al discloses the limitation of wherein generating the hash key comprises hashing the character string (random string) with the private key (secret string) (see column 7, lines 29-43).

As per claim 4, Bowman et al discloses wherein generating a character string comprises randomly generating the character string (see column 7, lines 25-29).

As per claim 5, Bowman et al discloses determining the private key (secret sting) at the recipient using the identification key (secret ID) (see column 9, lines 27-29); and decrypting the encrypted data at the recipient using the private key (secret sting) and the character string (random string) (see column 9, lines 29-35).

As per claim 6, Bowman et al discloses the limitation of wherein the recipient is adapted to access a relational database associating the identification key (secret ID) with the private key (secret sting) (see column 9, lines 27-29).

As per claim 7, Bowman et al discloses determining the private key (secret sting) at the recipient using the identification key (secret ID) (see column 9, lines 27-29); determining the hash key at the recipient using the private key (secret sting) and the character string (random string) (see column 9, lines 29-33); decrypting the encrypted data using the hash key (see column 9, lines 33-35).

As per claim 8, Bowman et al discloses wherein determining the hash key comprises hashing the character string (random string) with the private key (secret string) (see column 9, lines 29-34).

As per claim 11, Bowman et al teaches a method for secure data transmission, comprising:

receiving a character string (random string)from a sender (see column 8, lines 18-22);

receiving an identification key (secret ID) from the sender (see column 8, lines 18-22);

receiving encrypted data from the sender (see column 8, lines 18-22);

determining the private key (secret sting) associated with the sender using the identification key (secret ID) (see column 9, lines 27-29); and decrypting the encrypted data using the private key (secret sting) and the character string (random string) (see column 9, lines 29-35).

As per claim 12, Bowman et al discloses determining a hash key using the private key (secret sting) and the character string (random string) (see column 9, lines 29-33); and wherein decrypting the encrypted data comprises decrypting the encrypted data using the hash key (see column 9, lines 33-35).

As per claim 13, Bowman et al discloses wherein determining the private key comprises accessing a relational database associating the identification key (secret ID) with the private key (secret sting) (see column 9, lines 27-29).

As per claim 14, Bowman et al discloses wherein receiving a character string (random string) comprises receiving a randomly generated character string (see column 7, lines 25-29 and 57-61).

As per claim 15, Bowman et al discloses hashing the character string (random string) with the private key (secret sting) to generate a hash key (see column 9, lines 29-33); and wherein decrypting the encrypted data comprises decrypting the encrypted data using the hash key (see column 9, lines 33-35).

As per claim 16, Bowman et al discloses receiving a signature from the sender (see column 7, lines 59-67); and

verifying the signature using the decrypted data, the private key (secret sting), and the character string (random string) (see column 9, lines 29-55).

As per claim 17, Bowman et al discloses receiving a signature from the sender (see column 7, lines 59-67), determining a hash key using the private key (secret sting) and the character string (random string) (see column 9, lines 29-33); and

verifying the signature using the decrypted data and the hash key (see column 9, lines 29-55).

As per claim 19, Bowman et al teaches a system for secure data transmission, (see fig. 11) comprising: a processor; a memory coupled to the processor (see column 13, lines 10-39); a string generator stored in the memory and executable by the processor (see column 13, lines 10-39 and column 7, lines 25-29), the string generator adapted to generate a character string (see column 7, lines 25-29);

a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to generate a hash key (key (SHAD)) using the character string (random string) and a private key (secret string) (see column 7, lines 29-43); an encryption engine stored in the memory and executable by the processor, the encryption engine adapted to encrypt the data using the hash key (see column 7, lines 41-45) and wherein the processor is adapted to transmit the encrypted data (encrypted VBC), an identification key (secret ID) related to the private key (secret string), and the character string (random string) to a recipient (ee column 8, lines 18-22 and column 7, lines 57-62).

As per claim 21, Bowman et al discloses wherein the recipient is adapted to decrypt the encrypted data and verify the signature using the decrypted data (see, column 9, lines 33-55).

As per claim 22, Bowman et al discloses wherein the hashing engine is adapted to hash the character string (random string) with the private key (secret sting) to generate the hash key (see column 9, lines 29-33).

As per claim 23, Bowman et al discloses wherein the string generator is adapted to randomly generate the character string (random string) (see column 7, lines 28-29).

As per claim 24, Bowman et al discloses wherein the recipient is adapted to decrypt the encrypted data using the identification key (secret ID) and the character string (random string) (see column 9, lines 27-35).

As per claim 25, Bowman et al discloses wherein the recipient is adapted to determine the hash key using the identification key (secret ID) and the character string (random string) using the private key (secret sting) and the character string (random string) and decrypt the encrypted data using the hash key (see column 9, lines 27-35).

As per claim 26, Bowman et al discloses the limitation of wherein the recipient is adapted to access a relational database associating the identification key (secret ID) with the private key (secret sting) (see column 9, lines 27-29).

As per claim 27, Bowman et al teaches a system for secure data transmission, (see fig. 11) comprising: a processor adapted to receive encrypted data (encrypted VBC), an identification key (secret ID), and a character string (random string) from a sender (see column 8, lines 18-22); a memory coupled to the processor (see column 13, lines 10-39); a relational database stored in the memory and accessible by the processor, the relational database relating the identification key (secret ID) to a private key (secret sting) (see column 9, lines 27-29); a decryption engine stored in the memory and executable by the processor, (see column 13, lines 10-39), the decryption engine adapted to decrypt the encrypted data using the private key (secret sting) and the character string (random string) (see column 9, lines 29-35).

As per claim 28, Bowman et al discloses a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to generate a hash key using the character string (random string) and a private key (secret string) (see column 9, lines 29-35) and the decryption engine adapted to decrypt the encrypted data using the hash key (see column 9, lines 29-35).

As per claim 29, Bowman et al discloses comprising a signature engine (hash algorithm) stored in the memory and executable by the processor, the signature engine adapted to verify a signature received from the sender using the private key (secret sting), and the character string (random string) (see column 9, lines 29-55).

As per claim 30, Bowman et al discloses a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to generate a hash key using the private key (secret sting), and the character string (random string) (see column 9, lines 29-55); and a signature engine stored in the memory and executable by the processor, the signature engine adapted to verify a signature received from the sender using the hash key and the decrypted data (see column 9, lines 29-55).

As per claim 31, Bowman et al discloses a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to hash the character string (random string) with the private key (secret sting) to generate a hash key (see column 9, lines 29-55); and the decryption engine adapted to decrypt the encrypted data using the hash key (see column 9, lines 29-35).

As per claim 32, Bowman et al discloses a string generator stored in the memory and executable by the processor, the string generator adapted to generate a character string (random string) (see column 7, lines 25-29), and wherein the decryption engine is further adapted to encrypt data for transmitting to the sender using the character string (random string) and the private key (secret sting) (see column 9, lines 29-55 and column 11, line 65 through column 12, line 14).

As per claim 33, Bowman et al discloses a string generator stored in the memory and executable by the processor, the string generator adapted to generate a character string (random string) (see column 7, lines 25-29); a hashing engine stored in the memory and executable by the

processor, the hashing engine adapted to hash the character string (random string) with the private key (secret sting) to generate a hash key (see column 9, lines 29-55); and wherein the decryption engine is further adapted to encrypt data for transmitting to the sender using the hash key (see column 9, lines 29-55 and column 11, line 65 through column 12, line 14).

As per claim 34, Bowman et al discloses a signature engine stored in the memory and executable by the processor, the signature engine adapted to generate a first signature using the decrypted data and compare the first signature to a second signature received from the sender (see column 9, lines 29-55).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3, 9, 10, 18, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,751,736 to **Bowman et al.**

As per claim 3, Bowman et al substantially discloses generating a signature using the secret string (private key) and the data and transmitting the signature to the recipient (see column 7, lines 59-67). The difference between **Bowman et al** and the claimed invention is that Bowman et al uses the private key to generate the signature whereas the claimed invention uses the hash key. **Bowman et al** teaches the hash key is generated from the secret string (private key) and a random string (see column 7, lines 29-41), therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Bowman et al** to use the hash key instead of the private key to generate the signature for better security since it is harder for the recipient to be in possession of the hash key that needs to be regenerated using the secret string (private key) than it is for the recipient to determine the secret string (private key) (see column 8, lines 35-45); One of ordinary skill in the art would have recognized this advantage for using the hash key instead of the private key as suggested by **Bowman et al** it only requires an unlawful party to know the key that was used by the sender to duplicate the signature (see column 9, lines 50-55).

As per claim 9, Bowman et al substantially discloses generating a first signature by the sender using the secret string (private key) and the data and transmitting the first signature to the recipient (see column 7, lines 59-67). **Bowman et al** further discloses the recipient adapted to determine the hash key for decrypting the data and compare the first signature to a second signature generated by the recipient using the hash key and the decrypted data (see column 9, lines 29-55). The difference between **Bowman et al** and the claimed invention is that Bowman

et al uses the private key to generate the signature whereas the claimed invention uses the hash key. **Bowman et al** teaches the hash key is generated from the secret string (private key) and a random string (see column 7, lines 29-41), therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Bowman et al** to use the hash key instead of the private key to generate the signature for better security since it is harder for the recipient to be in possession of the hash key that needs to be regenerated using the secret string (private key) than it is for the recipient to determine the secret string (private key) (see column 8, lines 35-45); One of ordinary skill in the art would have recognized this advantage for using the hash key instead of the private key as suggested by **Bowman et al** it only requires an unlawful party to know the key that was used by the sender to duplicate the signature (see column 9, lines 50-55).

As per claim 10, Bowman et al substantially discloses generating a signature by the sender using the secret string (private key) and the data and transmitting the signature to the recipient (see column 7, lines 59-67). **Bowman et al** further discloses determining the private key (secret sting) at the recipient using the identification key (secret ID) (see column 9, lines 27-29); determining the hash key at the recipient using the private key (secret sting) and the character string (random string) (see column 9, lines 29-33); decrypting the encrypted data at the recipient using the hash key (see column 9, lines 33-35); and verifying the signature at the recipient using the hash key and the decrypted data (see column 9, lines 29-55). The difference between **Bowman et al** and the claimed invention is that Bowman et al uses the private key to generate the signature whereas the claimed invention uses the hash key. **Bowman et al** teaches

the hash key is generated from the secret string (private key) and a random string (see column 7, lines 29-41), therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Bowman et al** to use the hash key instead of the private key to generate the signature for better security since it is harder for the recipient to be in possession of the hash key that needs to be regenerated using the secret string (private key) than it is for the recipient to determine the secret string (private key) (see column 8, lines 35-45); One of ordinary skill in the art would have recognized this advantage for using the hash key instead of the private key as suggested by **Bowman et al** it only requires an unlawful party to know the key that was used by the sender to duplicate the signature (see column 9, lines 50-55).

As per claim 18, Bowman et al substantially discloses receiving a first signature from the sender (see column 7, lines 59-67); determining the hash key at the recipient using the private key (secret sting) and the character string (random string) (see column 9, lines 29-33); generating a second signature by the sender using the secret string (private key) and the decrypted data (see column 9, lines 33-50); and comparing the first signature to the second signature (see column 9, lines 43-50). **Bowman et al** further discloses the recipient adapted to determine the hash key for decrypting the data and compare the first signature to a second signature generated by the recipient using the hash key and the decrypted data (see column 9, lines 29-55). The difference between **Bowman et al** and the claimed invention is that Bowman et al uses the private key to generate the signature whereas the claimed invention uses the hash key. **Bowman et al** teaches the hash key is generated from the secret string (private key) and a random string (see column 7, lines 29-41), therefore, it would have been obvious to one of ordinary skill in the art at the time

the invention was made to modify **Bowman et al** to use the hash key instead of the private key to generate the signature for better security since it is harder for the recipient to be in possession of the hash key that needs to be regenerated using the secret string (private key) than it is for the recipient to determine the secret string (private key) (see column 8, lines 35-45); One of ordinary skill in the art would have recognized this advantage for using the hash key instead of the private key as suggested by **Bowman et al** it only requires an unlawful party to know the key that was used by the sender to duplicate the signature (see column 9, lines 50-55).

As per claim 20, Bowman et al discloses a signature engine (hash algorithm) stored in the memory and executable by the processor, (see column 13, lines 10-39) the signature engine adapted to generate a signature using the secret string (private key) and the data, the processor further adapted to transmit the signature to the recipient (see column 7, lines 59-67). The difference between **Bowman et al** and the claimed invention is that Bowman et al uses the private key to generate the signature whereas the claimed invention uses the hash key. **Bowman et al** teaches the hash key is generated from the secret string (private key) and a random string (see column 7, lines 29-41), therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Bowman et al** to use the hash key instead of the private key to generate the signature for better security since it is harder for the recipient to be in possession of the hash key that needs to be regenerated using the secret string (private key) than it is for the recipient to determine the secret string (private key) (see column 8, lines 35-45); One of ordinary skill in the art would have recognized this advantage for using the hash key instead

of the private key as suggested by **Bowman et al** it only requires an unlawful party to know the key that was used by the sender to duplicate the signature (see column 9, lines 50-55).

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure (see PTO-form 892).

4.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Carl Colin/
Patent Examiner, A.U. 2136
November 7, 2007